

FORM PTO-1082
TRANSMITTAL FOR NEW U.S. PATENT APPLICATION

Assistant Commissioner
for Patents
Washington, D.C. 20231

BOX APPLICATIONS

Re: New U.S. Patent Application
For: METHOD AND APPARATUS FOR
TRANSMITTING ENCRYPTION-RESULTANT
INFORMATION AND DECRYPTING INFORMATION
Inventor(s): Seiji HIGURASHI
Attorney Docket: 0102/0141

Sir:

Attached hereto is the application identified above, including 27 pages of textual specification including 8 claims, and 5 sheets of drawings.

The Government filing fee is calculated as follows:

(Col 1)		(Col 2)		(Col 3)	SMALL ENTITY		OR	NON-SMALL ENTITY	
TOTAL	NO. FILED			NO. EXTRA	RATE	FEE		RATE	FEE
	8	minus	20		x9=	0		x18=	\$
INDEP	7	minus	3	4	x40=	0		x80=	\$320
_ First Presentation, Multiple Dependent Claims					+135=	0		+270=	\$
Base Filing Fee						\$355			\$710
TOTAL FILING FEE* (accounting for possible small entity status)						\$	OR TOTAL		\$1030

☐ *Reduced by one-half, as applicant(s) is/are a "small entity". A Declaration Claiming Small Entity Status:

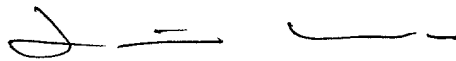
- ☐ is filed herewith;
☐ will be filed at a later date;
☐ was filed in the parent application.

☒ Foreign priority is claimed under 35 U.S.C. § 119 from Japanese Patent Application No.11-335502 dated November 26, 1999.

- ☐ Priority document(s) will be submitted at a later date.
☒ Priority document(s) is/are submitted herewith.

- ☐ There is no claim to foreign priority under 35 U.S.C. § 119.
- ☒ Executed Declaration(s) is/are submitted herewith.
- ☐ Executed Declaration(s) will be submitted at a later date pursuant to 37 CFR § 1.41 and § 1.53, with an appropriate surcharge under 37 CFR § 1.16(e).
- ☐ Formal drawing(s) is/are attached.
- ☒ Formal drawing(s) will be submitted at a later date.
- ☐ An Information Disclosure Statement, PTO-1449 and reference(s) cited therein is/are submitted.
- ☒ Assignment document(s) is/are submitted herewith, along with Form PTO-1595; the recordation fee of \$40.00 per document is enclosed herewith.
- ☒ A check in the amount of \$1,070.00 is enclosed. The Commissioner is hereby authorized to charge any deficiency under 37 CFR §§ 1.16 or 1.17, or credit any overpayment, to Deposit Account No. 50-0501. A duplicate copy of this form is attached.
- ☐ No payment is enclosed at this time. Full payment will be made when the executed Declaration is submitted.
- ☒ The Commissioner is hereby authorized to charge any fee deficiency, except the filing fee, *during the entire pendency of the present application*, or credit any overpayment, to Deposit Account No. 50-0501. A duplicate copy of this Form is enclosed.

Respectfully submitted,



Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
1901 N. Fort Myer Drive, Suite 501
Arlington, Virginia 22209
Phone: (703) 522-8872

Date: Oct 27 2000

- 1 -

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR TRANSMITTING ENCRYPTION-
RESULTANT INFORMATION AND DECRYPTING INFORMATION

BACKGROUND OF THE INVENTION5 Field of the Invention

This invention relates to a method of transmitting encryption-
resultant information and decrypting information. Also, this
invention relates to an apparatus for transmitting encryption-
resultant information and decrypting information. In addition, this
10 invention relates to a method of recording encryption-resultant
information and decrypting information on a recording medium.
Furthermore, this invention relates to an apparatus for recording
encryption-resultant information and decrypting information on a
recording medium. In addition, this invention relates to a
15 recording medium.

Description of the Related Art

It is known that original contents information is encrypted,
and the encryption-resultant information and also decrypting
information are recorded on an optical disc. Generally, the
20 encryption-resultant information is assigned to a main recording
area of the optical disc while the decrypting information is assigned
to a lead-in area thereof. Disc players reproduce the encryption-
resultant information and the decrypting information from the
optical disc. Only disc players owned by legitimate users are able to
25 decrypt the encryption-resultant information into the original
contents information in response to the decrypting information.

It is conceivable that encryption-resultant information and decrypting information are recorded on separate areas of a magnetic tape. In this conceivable case, the following problems arise. Access to the decrypting information takes a long time during playback.

- 5 There is some difficulty with playback from an intermediate point of the magnetic tape.

Also, it is conceivable that encryption-resultant information and decrypting information are recorded on a common area of a magnetic tape. In this conceivable case, a problem arises in the
10 synchronization between the encryption-resultant information and the decrypting information during playback. In addition, the following problems arise. It is necessary to provide a surplus memory. Signal processing up to decoding takes a long time.

SUMMARY OF THE INVENTION

- 15 It is a first object of this invention to provide an improved method of transmitting encryption-resultant information and decrypting information.

It is a second object of this invention to provide an improved apparatus for transmitting encryption-resultant information and
20 decrypting information.

It is a third object of this invention to provide an improved method of recording encryption-resultant information and decrypting information on a recording medium.

- It is a fourth object of this invention to provide an improved
25 apparatus for recording encryption-resultant information and decrypting information on a recording medium.

It is a fifth object of this invention to provide an improved recording medium.

A first aspect of this invention provides a method of transmitting information. The method comprises the steps of
5 transmitting an information signal containing 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information, the error correction code signal being for correction of at least one error in the encryption-resultant information, the error correction code signal being repetitively
10 completed at a completion period, the decrypting information being for decryption of the encryption-resultant information, the decrypting information being repetitively completed piece by piece; and dispersively placing at least one complete piece of the decrypting information in a portion of the information signal which
15 corresponds to the completion period of the error correction code signal.

A second aspect of this invention provides a method of recording information. The method comprises the steps of recording an information signal on a recording medium, the
20 information signal containing 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information, the error correction code signal being for correction of at least one error in the encryption-resultant information, the error correction code signal being repetitively completed at a completion period, the
25 decrypting information being for decryption of the encryption-resultant information, the decrypting information being repetitively

completed piece by piece; and dispersively placing at least one complete piece of the decrypting information in a portion of the information signal which corresponds to the completion period of the error correction code signal.

5 A third aspect of this invention provides a method of recording information. The method comprises the steps of recording a digital information signal on a recording medium, the digital information signal containing 1) decrypting information and 2) encryption resultants of video information and an error
10 correction code signal, the error correction code signal being repetitively completed at a completion period corresponding to one of a predetermined number of recording tracks and a predetermined number of recording sectors, the decrypting information being for decryption of the encryption resultants, the
15 decrypting information being repetitively completed piece by piece; and dispersively placing at least one complete piece of the decrypting information in a portion of the digital information signal which corresponds to the completion period of the error correction code signal.

20 A fourth aspect of this invention is based on the third aspect thereof, and provides a method wherein the recording medium comprises a magnetic tape.

 A fifth aspect of this invention provides a tape-like recording medium formed with tracks each having a predetermined number
25 of data blocks of a fixed length, segments of an information signal being recorded on respective data blocks in the tracks, the

information signal containing 1) decrypting information and 2) encryption resultants of video information and an error correction code signal, the error correction code signal being completed in every unit corresponding to a predetermined number of tracks, the
5 decrypting information being for decryption of the encryption resultants, the decrypting information being dispersively placed in the information signal so that the decrypting information is completed in every unit equal to the completion unit of the error correction code signal.

10 A sixth aspect of this invention provides an apparatus for transmitting information. The apparatus comprises means for transmitting an information signal containing 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information, the error correction code signal being for
15 correction of at least one error in the encryption-resultant information, the error correction code signal being repetitively completed at a completion period, the decrypting information being for decryption of the encryption-resultant information, the decrypting information being repetitively completed piece by piece;
20 and means for dispersively placing at least one complete piece of the decrypting information in a portion of the information signal which corresponds to the completion period of the error correction code signal.

A seventh aspect of this invention provides an apparatus for
25 recording information. The apparatus comprises means for recording an information signal on a recording medium, the

information signal containing 1) encryption-resultant information,
2) an error correction code signal, and 3) decrypting information,
the error correction code signal being for correction of at least one
error in the encryption-resultant information, the error correction
5 code signal being repetitively completed at a completion period, the
decrypting information being for decryption of the encryption-
resultant information, the decrypting information being repetitively
completed piece by piece; and means for dispersively placing at
least one complete piece of the decrypting information in a portion
10 of the information signal which corresponds to the completion
period of the error correction code signal.

An eighth aspect of this invention provides an apparatus
comprising means for generating decrypting information for
decryption of encryption-resultant information, the decrypting
15 information being repetitively completed; means for combining
main information and the decrypting information into composite
information, the main information containing the encryption-
resultant information and error correction code information, the
error correction code information being repetitively completed; and
20 means for synchronizing the repetitive completion of the decrypting
information and the repetitive completion of the error correction
code information in the composite information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a recording apparatus according to
25 a first embodiment of this invention.

Fig. 2 is a diagram of the format of one recording track on a

recording medium.

Fig. 3 is a diagram of the format of one data block (one sync block) in a main code area in Fig. 2.

Fig. 4 is a diagram of the format of first and second 1-byte address information pieces ID0 and ID1 in Fig. 3.

Fig. 5 is a diagram of the structure of one pack.

Fig. 6 is a block diagram of a reproducing apparatus in the first embodiment of this invention.

Fig. 7 is a block diagram of a descrambling unit in Fig. 6.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

First Embodiment

Fig. 1 shows a recording apparatus according to a first embodiment of this invention. The recording apparatus in Fig. 1 includes a scrambler (an encryptor) 51. The scrambler 51 receives an input MPEG2 transport stream. Also, the scrambler 51 receives key information from a suitable device (not shown). The device 51 scrambles (encrypts) the input MPEG2 transport stream in response to the key information. The scrambler 51 outputs the scrambling-resultant MPEG2 transport stream to a D-VHS encoder 54.

A signal generator 55 receives the key information. Also, the signal generator 55 receives version information and check information from suitable devices (not shown). The signal generator 55 produces pack information in response to the key information, the version information, and the check information. The signal generator 55 outputs the pack information to the D-VHS encoder

54. The pack information contains decrypting information. The decrypting information has pieces equal to or corresponding to the key information, the version information, and the check information respectively. The decrypting information can be updated, for
5 example, 30 bytes by 30 bytes. In other words, the decrypting information can be repetitively completed 30 bytes by 30 bytes. In this case, every 30-byte piece of the decrypting information is a unit.

Thus, the decrypting information can be repetitively
10 completed piece by piece. Every complete piece of the decrypting information corresponds to, for example, 30 bytes.

A signal generator 56 produces main header information. The signal generator 56 outputs the main header information to the D-VHS encoder 54.

15 The D-VHS encoder 54 encodes and multiplexes the scrambling-resultant MPEG2 transport stream, the pack information, and the main header information into a signal of the D-VHS format. As previously mentioned, the pack information contains the decrypting information. The D-VHS encoder 54
20 outputs the D-VHS signal to a recording amplifier 57. The device 57 amplifies the D-VHS signal. The amplification-resultant signal is transmitted from the recording amplifier 57 to magnetic heads 58 and 59 via rotary transformers (not shown). The magnetic heads 58 and 59 periodically and alternately record the amplification-
25 resultant signal, that is, the output signal of the recording amplifier 57, on a magnetic tape 60.

The magnetic heads 58 and 59 differ from each other in azimuth angle. The magnetic heads 58 and 59 are mounted on the circumferential surface of a rotary drum 61. The rotary drum 61 is rotated by a suitable servo mechanism (not shown). The magnetic
5 heads 58 and 59 rotate together with the rotary drum 61. The magnetic heads 58 and 59 are diametrically opposed to each other. In other words, the magnetic heads 58 and 59 are spaced by an angular interval of 180 degrees. The magnetic tape 60 is wrapped on the circumferential surface of the rotary drum 61 in an angular
10 range of about 180 degrees along a part of helix. A suitable mechanism (not shown) feeds the magnetic tape 60 relative to the rotary drum 61 at a constant speed. Recording tracks are successively formed on the magnetic tape 60 while the output signal of the recording amplifier 57 is recorded alternately by the
15 magnetic heads 58 and 59. The recording tracks are slant with respect to the longitudinal direction of the magnetic tape 60.

Each recording track on the magnetic tape 60 is composed of equal-size data blocks sequentially arranged in the direction of the scanning by the magnetic head 58 or 59. The data blocks are also
20 referred to as the sync blocks (SB). As shown in Fig. 2, one recording track has a sequence of a front margin area 21 of 2 sync blocks, a preamble area 22 of 3 sync blocks, a sub code area 23 of 4 sync blocks, a post-amble area 24 of 3 sync blocks, an IBG area 25 of 3 sync blocks, a preamble area 26 of 1 sync block, a main code area
25 (data area) 27 of 336 sync blocks, a post-amble area 28 of 2 sync blocks, and a rear margin area 29. The main code area 27 and the

sub code area 23 can be used as information recording areas.

The speed of rotation of the rotary drum 61 can be changed by the servo mechanism between 30 rps and 29.97 rps. A "1.001" flag indicates whether the speed of rotation of the rotary drum 61 is
5 equal to 30 rps or 29.97 rps. In the case where the "1.001" flag is in a state of "0", the rear margin area 29 is composed of 2 sync blocks. Thus, in this case, each recording track is formed by 356 sync blocks. In the case where the "1.001" flag is in a state of "1", the rear margin area 29 is composed of 2.356 sync blocks. Thus, in
10 this case, each recording track is formed by 356.356 sync blocks. The sub code area 23 has a fixed length of 4 sync blocks and the main code area 27 has a fixed length of 336 sync blocks regardless of the state of the "1.001" flag. For example, each of 188-byte
15 packets in the MPEG2 transport stream is recorded on two adjacent sync blocks in the main code area 27.

As shown in Fig. 3, each of the sync blocks in the main code area 27 corresponds to 112 bytes in capacity (size), and has a sequence of sub areas 31, 32, 33, 34, 35, and 36. The first sub area 31 has 2 bytes, and stores a sync signal for enabling the present
20 sync block to be reproduced. The second sub area 32 has 3 bytes, and stores address information composed of three 1-byte pieces ID0, ID1, and ID3 sequentially arranged in that order. The address information is also referred to as the identification (ID) information. The third sub area 33 has 2 bytes, and stores main header
25 information composed of information pieces of different types. The fourth sub area 34 has 1 byte. The fourth sub area 34 is an auxiliary

data (DATA-AUX) area. The fifth sub area 35 has 96 bytes, and stores effective data or real data. The fifth sub area 35 is also referred to as the data storing area 35. The sixth sub area 36 has 8 bytes, and stores an inner code signal or a signal of inner parities for
5 correcting an error or errors in the information represented by the present sync block (the information represented by other sub areas, for example, the sub areas 31-35 or 33-35).

The third, fourth, and fifth sub areas 33, 34, and 35 form a 99-byte data area in which the latter 96 bytes compose the data
10 storing area 35 assigned to effective information or real information. In the main-header storing area or the third sub area 33, format information is assigned to 4 higher bits in the first byte, and sync block information is assigned to 12 bits, that is, 4 lower bits in the first byte plus 8 bits in the second byte.

15 In the second sub area 32, the 1-byte address information piece ID2 is an error-correction parity signal for the 1-byte address information pieces ID0 and ID1. As shown in Fig. 4, 4 higher bits (bit "7" to bit "4") in the address information piece ID0 represent a sequence number 41, and 3 intermediate bits (bit "3" to bit "1")
20 therein represent a track pair number 42. The lowest bit (bit "0") in the address information piece ID0 and 8 bits (bit "7" to bit "0") in the address information piece ID1 represent a sync block number 43. Thus, 9 bits represent the sync block number 43.

The sequence number 41 depends on the period of the
25 record signal and the repetition of an error correction code (ECC) signal. The error correction code (ECC) signal means an ECC-

encoding-resultant signal containing a main information signal, an inner parity signal, and an outer parity signal. The error correction code signal is repetitively completed 6 tracks by 6 tracks.

Accordingly, the sequence number 41 is incremented by "1" per 6
5 tracks. The signal recording period corresponds to 24 tracks.

Accordingly, the sequence number 41 is reset to the initial value at a period of 24 tracks, and varies through one cycle for every time interval of 24 tracks.

Main data (for example, video data) and an outer code signal
10 or a signal of outer parities compose the error correction code signal. As previously mentioned, the error correction code signal is repetitively completed 6 tracks by 6 tracks. The outer parity signal is shuffled 180 sync blocks by 180 sync blocks. Six sets of 30 (180 sync blocks divided by 6 tracks) outer-parity sync blocks resulting
15 from every shuffle are placed in the main code areas 27 of 6 successive tracks respectively. Therefore, each main code area 27 stores 306 sync blocks loaded with the main data (for example, video data) and 30 sync blocks loaded with the outer parity signal. Every complete piece of the error correction code signal, that is,
20 every piece of the error correction code signal which corresponds to 6 tracks, has 2,016 (336 multiplied by 6) sync blocks.

The track pair number 42 reflects the repetition of the error correction code signal. As previously mentioned, recording tracks are successively formed on the magnetic tape 60 while the output
25 signal of the recording amplifier 57 is recorded alternately by the magnetic heads 58 and 59. Therefore, recording tracks relating to

a first azimuth angle alternate with recording tracks relating to a second azimuth angle different from the first azimuth angle. A common track pair number 42 is assigned to each of adjacent first-azimuth and second-azimuth tracks. As previously mentioned, the error correction code signal is repetitively completed 6 tracks by 6 tracks. Thus, the track pair number 42 cyclically varies as "0→1→2→0→..." in decimal notation. Specifically, a track pair number of "0" is assigned to a first pair of adjacent tracks. A track pair number of "1" is assigned to a second pair of adjacent tracks which follows the first pair. A track pair number of "2" is assigned to a third pair of adjacent tracks which follows the second pair. Then, a track pair number of "0" is assigned to a fourth pair of adjacent tracks which follows the third pair. This assignment of track pair numbers is iterated. Preferably, the track pair number 42 is represented by a binary code. In every pair, one track is discriminated from the other track on the basis of the difference between the azimuth angles.

The sync block number 43 indicates the arrangement order number of the present sync block among 336 sync blocks in the main code area 27.

The error correction code signal has components formed by inner parity signals (inner code signals) and outer parity signals (outer code signals). In every track (see Fig. 2), sync blocks extend over not only the main code area 27 but also the other areas 21-26, 28, and 29. Each sync block contains an inner parity signal (corresponding to the inner parity signal 36 in Fig. 3). Each sync

block contains data whose errors can be corrected in response to the inner parity signal and an outer parity signal. Segments of the previously-mentioned error correction code signal which has a completion period of 6 tracks are distributed to only sync blocks in the main code areas 27, and are not assigned to sync blocks in the other areas 21-26, 28, and 29.

The decrypting information is repetitively completed 6 tracks by 6 tracks in synchronism with the error correction code signal having a completion period of 6 tracks. Each complete piece, that is, each 6-track-corresponding piece, of the decrypting information is assigned to the main code areas 27 of six successive tracks. This design enables a reproducing side to decode the decrypting information simultaneously with the decoding of the main data (for example, video data) in the main code areas 27. Furthermore, the error rate of the main data (for example, video data) in the main code areas 27 and the error rate of the decrypting information therein can be equalized to each other so that efficient information reproduction can be implemented.

As previously mentioned, the main code area 27 (see Fig. 2) in each track has 336 sync blocks of the format in Fig. 3. Each sync block in the main code area 27 has a 1-byte auxiliary data (DATA-AUX) area 34. The D-VHS encoder 54 is designed so that the pack information which contains the decrypting information will be recorded on the auxiliary data (DATA-AUX) areas 34 in selected ones of the sync blocks in the main code area 27 as a pack form.

With reference to Fig. 5, the auxiliary data (DATA-AUX) areas

34 are separated into 6-byte groups loaded with 6-byte packs having a period corresponding to 6 sync blocks. Specifically, each group corresponding to one pack has the auxiliary data (DATA-AUX) areas 34 in six successive sync blocks. In each group (each pack), a pack header PC0 is recorded on the auxiliary data (DATA-AUX) area 34 in the first sync block $6n$, and pack pieces PC1, PC2, PC3, PC4, and PC5 following the pack header PC0 are recorded on the auxiliary data (DATA-AUX) areas 34 in the second, third, fourth, fifth, and sixth sync blocks $6n+1$, $6n+2$, $6n+3$, $6n+4$, and $6n+5$ respectively.

10 The pack header PC0 stores special information for identifying a time code, a program number, text data, TOC information, and decrypting information. Specifically, the pack header PC0 in which all of five higher bits are "1" indicates that the present pack stores a portion of the decrypting information or the
15 subsequent pack pieces PC1-PC5 store a portion of the decrypting information. In other words, the pack header PC0 in a state of "11111xxx" indicates that the present pack stores a portion of the decrypting information. In the pack header PC0 of the decrypting-information store pack, three lower bits represent a page number
20 which can change among 6 different values corresponding to 6 different pages respectively. Specifically, the page number can change among "000", "001", "010", "011", "100", and "101". Here, "pages" correspond to tracks, respectively.

 As previously mentioned, the decrypting information is
25 repetitively completed 6 tracks by 6 tracks, and every complete piece of the decrypting information is recorded on 6 successive

tracks. In more detail, every complete piece of the decrypting information is recorded on 6 packs (decrypting-information store packs) which extend in 6 successive tracks respectively. Thus, in every track, one is selected from among packs as a decrypting-
5 information store pack. Generally, every complete piece of the decrypting information has 30 bytes. Six 5-byte segments of every complete piece of the decrypting information are assigned to 6 packs (decrypting-information store packs) in 6 successive tracks, respectively. Thirty bytes of the six 5-byte segments are assigned,
10 respectively, to the thirty pack pieces PC1-PC5 in 6 decrypting-information store packs in 6 successive tracks. In this way, every complete piece of the decrypting information is dispersively recorded on 6 successive tracks. Therefore, the decrypting information is prevented from adversely affecting other pack
15 information. In addition, illegal recovery of the decrypting information is difficult.

The pack header PC0 of the decrypting-information store pack in first one of 6 successive tracks is in a state of "11111000". The pack header PC0 of the decrypting-information store pack in
20 second one of 6 successive tracks is in a state of "11111001". The pack header PC0 of the decrypting-information store pack in third one of 6 successive tracks is in a state of "11111010". The pack header PC0 of the decrypting-information store pack in fourth one of 6 successive tracks is in a state of "11111011". The pack header
25 PC0 of the decrypting-information store pack in fifth one of 6 successive tracks is in a state of "11111100". The pack header PC0

of the decrypting-information store pack in sixth one of 6 successive tracks is in a state of "11111101".

A reproducing side can detect every decrypting-information store pack by deciding whether all of five higher bits of a pack header PC0 are "1". The reproducing side can detect every group of 6 decrypting-information store packs loaded with one complete piece of the decrypting information by referring to the page numbers represented by the pack headers PC0. Accordingly, the reproducing side can detect every group of thirty pack pieces PC1-PC5 storing one complete piece of the decrypting information in response to the pack headers PC0.

The 6 different pages correspond 6 successive tracks in each group which stores one complete piece of the decrypting information. As previously mentioned, the decrypting information is recorded synchronously with the error correction code signal having a completion period of 6 tracks. This design enables a reproducing side to decode the decrypting information simultaneously with the decoding of the main data (for example, video data) in the main code areas 27. Furthermore, the error rate of the main data (for example, video data) in the main code areas 27 and the error rate of the decrypting information therein can be equalized to each other. In addition, the delay time of information processing can be minimized.

Complete pieces of the decrypting information which correspond to neighboring complete pieces of the error correction code signal are different or equal in contents.

Fig. 6 shows a reproducing apparatus according to the first embodiment of this invention. The recording apparatus in Fig. 1 and the reproducing apparatus in Fig. 6 may be combined into a single VTR or VCR.

5 In the reproducing apparatus of Fig. 6, magnetic heads 58 and 59 on a rotary drum 61 alternately scan a magnetic tape 60, and reproduce a signal therefrom. The reproduced signal is transmitted from the magnetic heads 58 and 59 to a reproducing amplifier 71 via rotary transformers (not shown). The device 71 amplifies the
10 reproduced signal. The reproducing amplifier 71 outputs the amplification-resultant signal to a D-VHS decoder 72. The device 72 decodes and demultiplexes the output signal of the reproducing amplifier 71 into an MPEG2 transport stream and pack information (a sequence of packs). The pack information comes from the
15 auxiliary data (DATA-AUX) areas 34 in selected ones of the 336 sync blocks composing the main code area 27 for every recording track. The D-VHS decoder 72 outputs the MPEG2 transport stream and the pack information to a descrambling unit (decrypting unit) 73.

As shown in Fig. 7, the descrambling unit 73 includes a
20 "11111" detector 73A, a fast-in fast-out register 73B, a key generator 73C, a descrambler (decryptor) 73D, and an extractor 73E.

The "11111" detector 73A receives the pack information (the sequence of packs) from the D-VHS decoder 72. The "11111"
25 detector 73A senses every pack in which all of five higher bits of the pack header PC0 are "1". Thus, the "11111" detector 73A senses

every decrypting-information store pack. Specifically, the "11111" detector 73A includes a comparator for deciding whether or not all of five higher bits of the pack header PC0 in every pack are "1". The "11111" detector 73A stores every sensed decrypting-information
5 store pack into the register 73B. Generally, 6 decrypting-information store packs simultaneously exist in the register 73B during a normal operation stage except an initial stage.

The key generator 73C accesses 6 decrypting-information store packs in the register 73B. The key generator 73C decides
10 whether or not the 6 accessed packs are in a common group for storing one complete piece of the decrypting information by referring to the pages represented by the pack headers PC0 of the packs. When the 6 accessed packs are in a common group, the key generator 73C reads out one complete piece of the decrypting
15 information from the pack pieces PC1-PC5 in the accessed packs. The key generator 73C reproduces or recovers the key information from the read-out complete piece of the decrypting information. The key generator 73C feeds the reproduced key information to the descrambler 73D.

20 The descrambler 73D receives the MPEG2 transport stream from the D-VHS decoder 72. The device 73D descrambles or decrypts the MPEG2 transport stream in response to the key information fed from the key generator 73C. The descrambler 73D outputs the descrambling-resultant MPEG2 transport stream (the
25 decrypting-resultant MPEG2 transport stream).

The extractor 73E receives the pack information (the

sequence of packs) from the D-VHS decoder 72. The extractor 73E separates the version information and the check information from the pack information. The extractor 73E outputs the version information and the check information. In general, the version
5 information and the check information are used in control of the reproducing apparatus.

It should be noted that the key generator 73C may be provided with a device for separating the version information and the check information from the complete piece of the decrypting
10 information. In this case, the extractor 73E is omitted from the descrambling unit 73.

Second Embodiment

A second embodiment of this invention is a modification of the first embodiment thereof. The second embodiment of this
15 invention is directed to recording and reproducing apparatuses (for example, digital-signal recording and reproducing apparatuses) of types different from the D-VHS types.

Third Embodiment

A third embodiment of this invention is a modification of the
20 first embodiment thereof. The third embodiment of this invention is designed so that at least two complete pieces of the error correction code signal are recorded on 6 successive tracks.

Fourth Embodiment

A fourth embodiment of this invention is a modification of the
25 first embodiment thereof. The fourth embodiment of this invention is designed so that a signal is recorded and reproduced on and from

an optical disc or a magnetic disc. The error correction code signal and the decrypting information are recorded on the optical disc or the magnetic disc in a manner such that they are completed in every unit corresponding to a given number of sectors.

5

Fifth Embodiment

A fifth embodiment of this invention is a modification of the first embodiment thereof. The fifth embodiment of this invention is designed so that a signal of the formats in Figs. 2 and 3 which contains the error correction code signal and the decrypting
10 information is transmitted by an information processing apparatus such as a personal computer.

WHAT IS CLAIMED IS:

1. A method of transmitting information, comprising the steps of:

- 5 transmitting an information signal containing 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information, the error correction code signal being for correction of at least one error in the encryption-resultant information, the error correction code signal being repetitively
- 10 completed at a completion period, the decrypting information being for decryption of the encryption-resultant information, the decrypting information being repetitively completed piece by piece; and
- dispersively placing at least one complete piece of the
- 15 decrypting information in a portion of the information signal which corresponds to the completion period of the error correction code signal.

2. A method of recording information, comprising the steps of:

- 20 recording an information signal on a recording medium, the information signal containing 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information, the error correction code signal being for correction of at least one error in the encryption-resultant information, the error correction
- 25 code signal being repetitively completed at a completion period, the decrypting information being for decryption of the encryption-

resultant information, the decrypting information being repetitively completed piece by piece; and

dispersively placing at least one complete piece of the decrypting information in a portion of the information signal which corresponds to the completion period of the error correction code signal.

3. A method of recording information, comprising the steps of:
recording a digital information signal on a recording medium,
10 the digital information signal containing 1) decrypting information and 2) encryption resultants of video information and an error correction code signal, the error correction code signal being repetitively completed at a completion period corresponding to one of a predetermined number of recording tracks and a
15 predetermined number of recording sectors, the decrypting information being for decryption of the encryption resultants, the decrypting information being repetitively completed piece by piece; and

dispersively placing at least one complete piece of the
20 decrypting information in a portion of the digital information signal which corresponds to the completion period of the error correction code signal.

4. A method as recited in claim 3, wherein the recording
25 medium comprises a magnetic tape.

5. A tape-like recording medium formed with tracks each having a predetermined number of data blocks of a fixed length, segments of an information signal being recorded on respective data blocks in the tracks, the information signal containing 1) decrypting
5 information and 2) encryption resultants of video information and an error correction code signal, the error correction code signal being completed in every unit corresponding to a predetermined number of tracks, the decrypting information being for decryption of the encryption resultants, the decrypting information being dispersively
10 placed in the information signal so that the decrypting information is completed in every unit equal to the completion unit of the error correction code signal.

6. An apparatus for transmitting information, comprising:
15 means for transmitting an information signal containing 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information, the error correction code signal being for correction of at least one error in the encryption-resultant information, the error correction code signal being
20 repetitively completed at a completion period, the decrypting information being for decryption of the encryption-resultant information, the decrypting information being repetitively completed piece by piece; and
means for dispersively placing at least one complete piece of
25 the decrypting information in a portion of the information signal which corresponds to the completion period of the error correction

code signal.

7. An apparatus for recording information, comprising:
means for recording an information signal on a recording
5 medium, the information signal containing 1) encryption-resultant
information, 2) an error correction code signal, and 3) decrypting
information, the error correction code signal being for correction of
at least one error in the encryption-resultant information, the error
correction code signal being repetitively completed at a completion
10 period, the decrypting information being for decryption of the
encryption-resultant information, the decrypting information being
repetitively completed piece by piece; and
means for dispersively placing at least one complete piece of
the decrypting information in a portion of the information signal
15 which corresponds to the completion period of the error correction
code signal.
8. An apparatus comprising:
means for generating decrypting information for decryption of
20 encryption-resultant information, the decrypting information being
repetitively completed;
means for combining main information and the decrypting
information into composite information, the main information
containing the encryption-resultant information and error
25 correction code information, the error correction code information
being repetitively completed; and

ABSTRACT OF THE DISCLOSURE

An information signal is transmitted. The information signal contains 1) encryption-resultant information, 2) an error correction code signal, and 3) decrypting information. The error correction code signal is designed for correction of at least one error in the encryption-resultant information. The error correction code signal is repetitively completed at a completion period. The decrypting information is designed for decryption of the encryption-resultant information. The decrypting information is repetitively completed piece by piece. At least one complete piece of the decrypting information is dispersively placed in a portion of the information signal which corresponds to the completion period of the error correction code signal.

FIG. 1

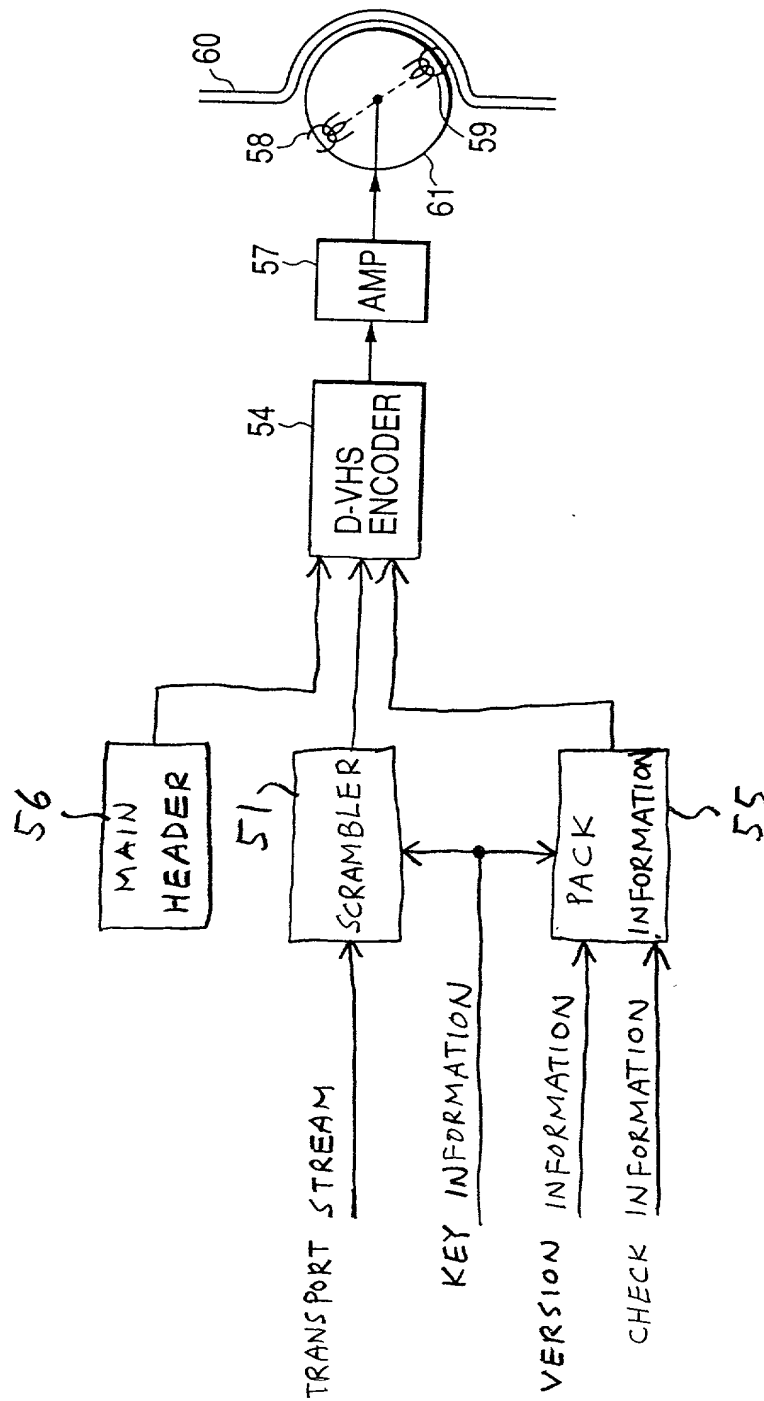


FIG. 2

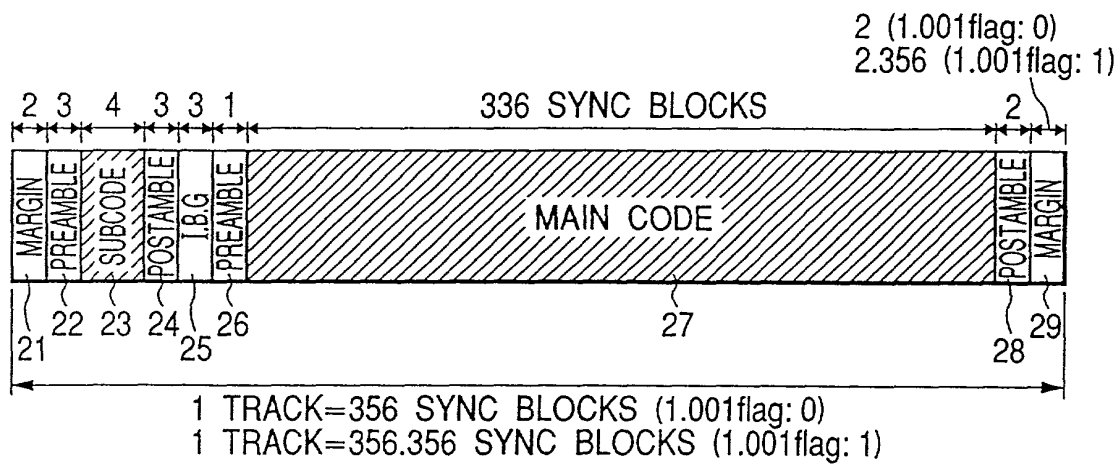


FIG. 3

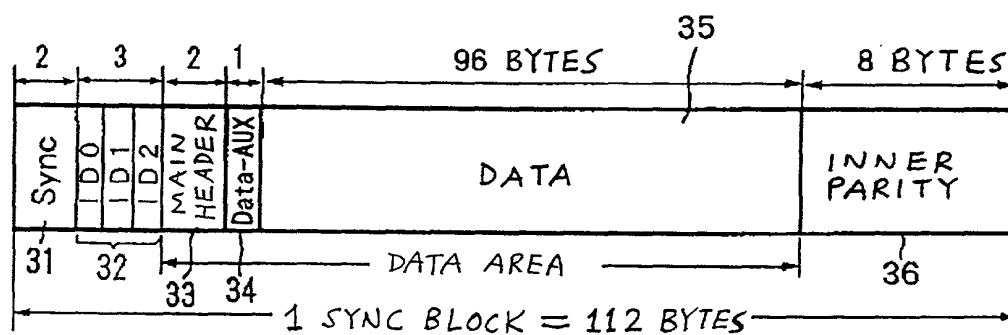


FIG. 4

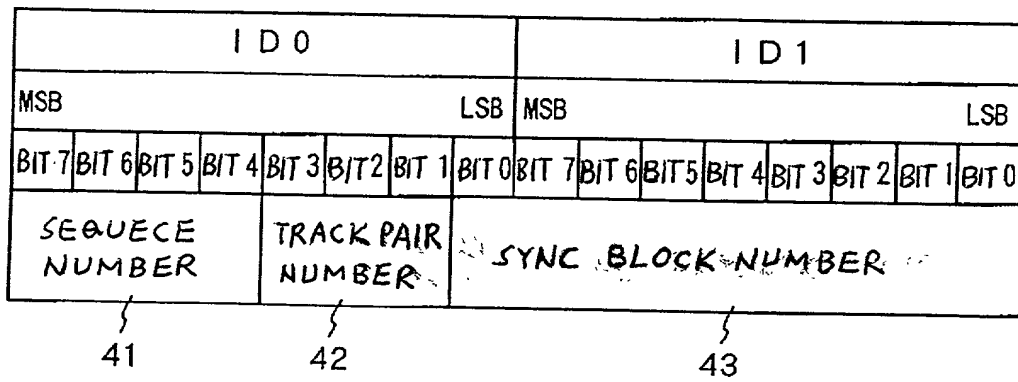


FIG. 5

SB #	CONTENTS
6 n	PC 0 (1111.1xxx)
6 n + 1	PC 1
6 n + 2	PC 2
6 n + 3	PC 3
6 n + 4	PC 4
6 n + 5	PC 5

FIG. 6

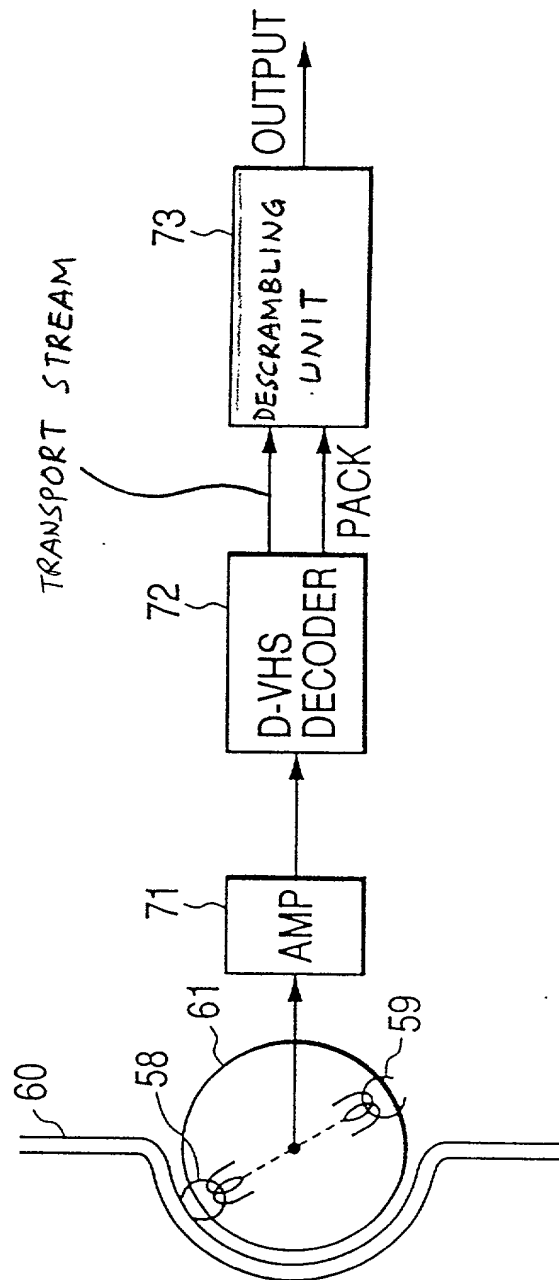
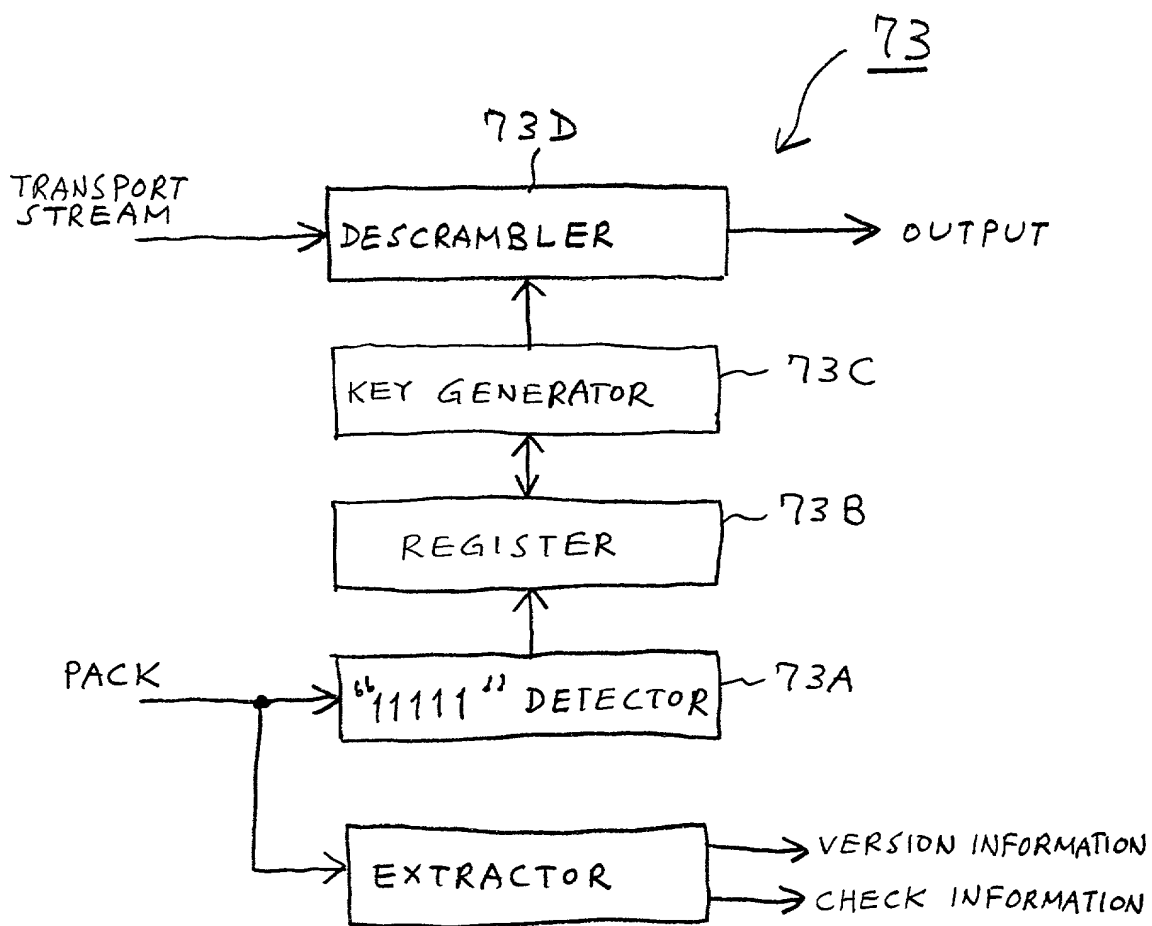


FIG. 7



DECLARATION AND POWER OF ATTORNEY

p000516 US
04-0017-TH
U.S.A.

Attorney Ref. No.

As a below-named inventor, I hereby declare: My residence, post office address and citizenship are as stated below next to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND APPARATUS FOR TRANSMITTING ENCRYPTION-RESULTANT INFORMATION AND DECRYPTING INFORMATION, the specification of which

(Check one)

☒ is attached hereto.☐ was filed on _____ as Application Serial No. _____

and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above, and acknowledge a duty to disclose information which is material to the examination of this application under 37 CFR 1.56(a). I hereby claim priority benefits under 35 U.S.C. 119 based on any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate on the present invention, filed before the application(s) on which priority is claimed.

FOREIGN APPLICATION(S), IF ANY, REFERRED TO ABOVE			
COUNTRY	APPLICATION NUMBER	DATE	PRIORITY CLAIMED
Japan	11-335502	November 26, 1999	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
			YES <input type="checkbox"/> NO <input type="checkbox"/>
			YES <input type="checkbox"/> NO <input type="checkbox"/>

I hereby claim benefit under 35 U.S.C. 120 of any U.S. application(s) listed below. If the subject matter of any claim(s) of this application is not disclosed in the prior U.S. application(s) as required by paragraph one of 35 U.S.C. 112. I acknowledge as duty to disclose material information as defined in 37 C.F.R. 1.56(a) regarding occurrences between the filing date of the prior application(s) and the national or PCT international filing date of this application.

APPLICATION SERIAL NUMBER	DATE	STATUS

I hereby appoint Louis Woo, RN 31,730 and Robert R. Priddy, RN 20,169 as my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

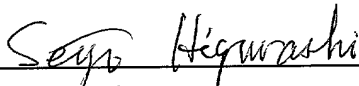
Address all communications to **LAW OFFICES OF LOUIS WOO, 1901 North Fort Myer Drive, Suite 501, Arlington, Virginia 22209**

All statements made herein of my own knowledge are true. All statements made on information and belief are believed to be true. These statements were made with knowledge that willful false statements and the like so made are punishable by fine, imprisonment, or both, under 18 U.S.C. 1001 and may jeopardize the validity of the application or any patent issuing thereon.

Note: Please sign one full given name and your surname, using initials where appropriate for other names. It is important that the name be consistent throughout the application papers. Signing of an application more than five weeks prior to filing or an undated application is not acceptable to the Patent and Trademark Office except for receiving an initial filing date.

1. Full name of inventor Seiji Higurashi Date: October 11, 2000

Inventor's signature



Residence Fuchu-shi, Tokyo, Japan

Citizenship Japanese

Post Office Address 1-36-7, Midori-cho, Fuchu-shi, Tokyo, Japan

[] Additional inventors listed